



## Daily Open Source Infrastructure Report 18 September 2015

### Top Stories

- Officials announced September 14 that 5 cooling towers, power lines, and communications at the Geysers geothermal power generation facility were damaged due to the Valley Fire in California. – *Los Angeles Times* (See item [3](#))
- General Motors Co announced September 17 that it would pay \$900 million and admit fault to resolve a U.S. criminal investigation into the company's handling of defective ignition switches in its vehicles and failure to disclose the defect to customers. – *Reuters* (See item [4](#))
- Crews worked September 17 to contain the 73,700-acre Valley Fire burning in California that destroyed 585 houses and caused 3 deaths. – *KRON 4 San Francisco* (See item [18](#))
- Researchers confirmed that the Chinese hacking group Iron Tiger stole data from U.S. defense contractors, intelligence agencies, FBI-based partners, other government entities, and tech-based contractors in multiple industries. – *Forbes* (See item [20](#))

---

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

#### SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

#### SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL and STATE

- [Government Facilities](#)
  - [Emergency Services](#)
-

## Energy Sector

1. *September 16, Caspar Star-Tribune* – (Wyoming) **Crews extinguish Douglas oil well fire.** Crews capped the final 3 burning wells September 15 at a Chesapeake Energy oil site near Douglas, Wyoming, after the fire began September 6 and spread to all 6 wells at the site. The company is investigating the cause of the blaze.  
Source: [http://trib.com/news/state-and-regional/crews-extinguish-douglas-well-fire/article\\_901d301e-e6e2-5b45-ad32-94c62a75da57.html](http://trib.com/news/state-and-regional/crews-extinguish-douglas-well-fire/article_901d301e-e6e2-5b45-ad32-94c62a75da57.html)
2. *September 16, Associated Press* – (International) **State fines international oil and gas company over \$220K for fracking-well fire in Ohio.** The Ohio Environmental Protection Agency and Department of Natural Resources cited several violations and issued a \$223,000 fine against Norway-based Statoil September 15 after a June 2014 fire the company's natural gas fracking well in Monroe County forced evacuations and killed about 70,000 fish. An apparent tubing malfunction caused the fire and authorities stated that operations at the well pad can resume after fines are paid.  
Source:  
<http://www.dailyjournal.net/view/story/300e99169be0489982a9cfabd06ffdf4/OH--Gas-Well-Fire-Company-Fined>
3. *September 14, Los Angeles Times* – (California) **Northern California Valley fire damages part of huge geothermal power generator.** Houston-based Calpine announced September 14 that five cooling towers, power lines, and communications at the Geysers geothermal power generation facility along the Sonoma County and Lake County borders were damaged due to the Valley Fire burning in northern California. Officials reported that the damage did not impact services.  
Source: <http://www.latimes.com/local/lanow/la-me-ln-valley-fire-damages-part-of-huge-geothermal-power-generator-20150914-story.html>

For another story, see item [20](#)

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

See item [20](#)

## Critical Manufacturing Sector

4. *September 17, Reuters* – (National) **GM to pay \$900 million to end U.S. criminal ignition switch probe.** General Motors Co (GM) announced it would pay \$900 million September 17 and admit fault to resolve a U.S. criminal investigation into the company's handling of defective ignition switches in its vehicles and allegations that GM failed to disclose the defect and misled customers and the government about the safety of affected models. GM also agreed to a \$575 million partial settlement in

separate nationwide private and shareholder litigation.

Source: <http://www.reuters.com/article/2015/09/17/us-gm-probe-idUSKCN0RG2WF20150917>

## **Defense Industrial Base Sector**

See item [20](#)

## **Financial Services Sector**

5. *September 17, Help Net Security* – (International) **New POS trojan created by mixing code from older malware.** Security researchers from Dr. Web discovered a new trojan dubbed Trojan.MWZLesson, targeting point-of-sale (PoS) terminals to obtain bank card data from the device's compromised random access memory (RAM), that was pieced together with parts of the Neutrino backdoor and the Dexter PoS trojan. The malware can update itself, download and execute files, find documents, and mount HyperText Transport Protocol (HTTP) Flood attacks.  
Source: [http://www.net-security.org/malware\\_news.php?id=3101](http://www.net-security.org/malware_news.php?id=3101)
6. *September 16, Bloomberg News* – (New York) **Ex-Morgan Stanley broker pleads guilty to insider training.** A former broker for Morgan Stanley pleaded guilty to charges of insider trading on insider information stolen from Simpson, Thacher & Bartlett LLP, and to fraud charges alleging he bought securities for himself, his family, his friends and business partners, gaining \$5.6 million in profit from 2009 - 2013.  
Source: <http://www.bloomberg.com/news/articles/2015-09-16/ex-morgan-stanley-broker-pleads-guilty-in-insider-trading-case>
7. *September 16, Reuters* – (National) **CVS Health in \$48 million settlement of lawsuit over hiding loss.** CVS Health Corp agreed to pay \$48 million to resolve charges accusing the company of fraudulently concealing a \$4.5 billion loss of annual revenue in its pharmacy benefits manager business, leading to a dip in stock price on November 2009.  
Source: <http://www.reuters.com/article/2015/09/16/cvs-health-settlement-idUSL1N11M12K20150916>
8. *September 16, Los Angeles Times* – (California) **Two arrested in alleged \$21 million movie investment scheme.** A former insurance agent and a director were arrested on charges accusing them of a movie investment Ponzi scheme that cost more than 140 victims about \$21 million, in which they allegedly solicited investors for funding for fake films through Windsor Pictures LLC, while promising returns.  
Source: <http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-movie-investment-scam-20150916-story.html>

## **Transportation Systems Sector**

9. *September 17, KOTV 6 Tulsa* – (Alabama) **American Airlines jet makes emergency landing in Tulsa.** An American Airlines flight traveling from Dallas to St. Louis made

an emergency landing at Tulsa International Airport September 16 after the pilot reported smoke in the cockpit. Emergency crews inspected the plane and the flight resumed its course shortly after.

Source: <http://www.newson6.com/story/30052486/jet-flying-from-dallas-to-st-louis-makes-emergency-landing-in-tulsa>

10. *September 16, KNBC 4 Los Angeles* – (California) **91 Freeway lanes shut down near Corona due to storm damage.** Westbound lanes of 91 Freeway near Corona were shut down September 16 while crews conducted emergency road work following a September 15 rain storm that may have eroded part of the road. Officials reported major delays were expected in nearby areas.

Source: <http://www.nbclosangeles.com/news/local/91-Freeway-Lanes-Shut-Down-Near-Corona-Due-to-Storm-Damage-327838441.html>

11. *September 16, KSBY 6 San Luis Obispo*– (Oregon) **Alaska Airlines flight bound for Santa Barbara makes emergency landing.** An Alaska Airlines flight headed from Portland to Santa Barbara made an emergency landing in Rogue Valley International Medford Airport September 16 after smoke was found in the cargo hold. As a precaution, all 60 passengers were evacuated from the plane.

Source: <http://www.ksby.com/story/30049816/alaska-airlines-flight-bound-for-santa-barbara-makes-emergency-landing>

For another story, see item [20](#)

## **Food and Agriculture Sector**

12. *September 16, WUSA 9 Washington, D.C.* – (Washington, D.C.) **Downtown DC restaurant to reopen after dozens sickened.** The District of Columbia Department of Health (DOH) reported September 16 that Fig & Olive restaurant in downtown D.C. reopened after being closed for 6 days following a Salmonella outbreak that sickened 60 people and prompted the investigation of an additional 150 possible cases. DOH ordered the restaurant to address 16 violations, including absence of a written policy to manage foodborne illness.

Source: <http://www.wusa9.com/story/news/local/dc/2015/09/16/fig-and-olive-salmonella-outbreak-reopened/32511089/>

13. *September 16, U.S. Food and Drug Administration* – (National) **Karoun Dairies, Inc. issues nationwide voluntary recall of various cheeses because of possible health risk.** The U.S. Food and Drug Administration reported September 16 that San Fernando, California-based Karoun Dairies, Inc., is voluntarily recalling a variety of cheese products vacuumed packed in jars or in pails due to possible contamination with *Listeria monocytogenes*. The products were sold nationwide under the following brands: Karoun, Arz, Gopi, Queso Del Velle, Central Valley Creamery, Copi, and Yanni.

Source: <http://www.fda.gov/Safety/Recalls/ucm462976.htm>

## **Water and Wastewater Systems Sector**

14. *September 16, KSAL 1150 AM Salina* – (Kansas) **Boil water advisory for Minneapolis.** The Kansas Department of Health and Environment issued a boil advisory September 16 for the public water supply in Ottawa County due to a loss of pressure after a water main broke. Officials reported that the advisory will be in effect until pressure is restored and all other conditions are deemed resolved.  
Source: <http://www.ksal.com/boil-water-advisory-for-minneapolis/>

## **Healthcare and Public Health Sector**

15. *September 17, NJ.com* – (New Jersey) **Hospital worker admits selling more than 250 patient records.** A former billing supervisor at a Bergen County hospital pleaded guilty September 16 to selling over 250 patient records containing patient's personal information, including Social Security numbers and medical insurance information to an unnamed individual for cash.  
Source: [http://www.nj.com/passaic-county/index.ssf/2015/09/hospital\\_billing\\_supervisor\\_admits\\_selling\\_patient.html](http://www.nj.com/passaic-county/index.ssf/2015/09/hospital_billing_supervisor_admits_selling_patient.html)

## **Government Facilities Sector**

16. *September 17, Salt Lake City Deseret News* – (Utah) **Firefighter, Clearfield High teacher hospitalized after exposure to unknown gas.** A firefighter and a teacher from Clearfield High School in Utah were hospitalized September 16 after the teacher was sprayed with an unknown liquid and gas combination from a canister during class, which prompted the evacuation of approximately 300 students and the on-site treatment of 21 others due to potential exposure.  
Source: <http://www.deseretnews.com/article/865636968/Firefighter-Clearfield-High-teacher-hospitalized-after-exposure-to-unknown-gas.html?pg=all>
17. *September 17, Columbus Dispatch* – (Ohio) **Power outage cancels classes at Columbus State today.** Officials announced that power was restored and classes at Columbus State Community College, its Delaware campus, and 5 learning centers around central Ohio were cancelled September 17 after a September 16 power outage knocked out online systems before crews restored service, preventing access to homework assignments and communication with teachers.  
Source: <http://www.dispatch.com/content/stories/local/2015/09/17/columbus-state-cancels-classes-system-wide-due-to-power-outage.html>
18. *September 17, KRON 4 San Francisco* – (California) **Valley Fire: Body of missing reporter found; death toll rises to three.** Crews worked September 17 to contain the 73,700-acre Valley Fire burning in North Bay that destroyed 585 houses and caused 3 deaths.  
Source: <http://kron4.com/2015/09/17/valley-fire-day-6-of-the-fight-against-the-deadly-firestorm/>
19. *September 16, Duluth News Tribune* – (Wisconsin) **UWS dorm, Superior High**

**School evacuated after suspicious package found.** Police cleared the scene after evacuations of Superior High School and Ross-Hawes Hall at the University of Wisconsin-Superior lasted nearly 8 hours September 16 following the discovery of a newspaper-wrapped package found atop a sewer cover near a parking lot at the dormitory. The package was deemed safe after authorities determined it contained spoiled meat.

Source: <http://www.duluthnewstribune.com/news/3840447-uws-dorm-superior-high-school-evacuated-after-suspicious-package-found>

For additional stories, see items [20](#) and [22](#)

## **Emergency Services Sector**

Nothing to report

## **Information Technology Sector**

20. *September 17, Forbes* – (International) **Chinese-based cyber attacks on US military are ‘advanced, persistent and ongoing’: Report.** Trend Micro released research confirming that the Chinese advanced persistent threat (APT) group dubbed Iron Tiger was observed stealing trillions of bytes of data from U.S. defense contractors, intelligence agencies, FBI-based partners, other government entities, and tech-based contractors in the electric, aerospace, intelligence, telecommunications, energy, and nuclear engineering industries, including Westinghouse Electric Company. The group is believed to be an iteration of Emissary Panda/Threat Group 3390, who previously focused on east-Asian political targets.  
Source: <http://www.forbes.com/sites/lisabrownlee/2015/09/17/chinese-cyber-attacks-on-us-military-interests-confirmed-as-advanced-persistent-and-ongoing/>
21. *September 17, Help Net Security* – (International) **80% increase of malware on Windows devices.** Alcatel-Lucent released report findings revealing that 80 percent of mobile network malware infections detected in the first half of 2015 were found on Windows-based systems, that 10 of the largest threats on smartphones were mobile spyware, and that the prevalence of adware has been increasing, among other findings.  
Source: [http://www.net-security.org/malware\\_news.php?id=3102](http://www.net-security.org/malware_news.php?id=3102)
22. *September 17, The Register* – (International) **Malware links Russians to 7-year global cyberspy campaign.** Security researchers from F-Secure released new analysis revealing that the group behind the Dukes 7-year cyber-espionage malware campaign has been utilizing unique malware toolsets to steal information from governments worldwide as well as non-government organizations (NGOs). Researchers believe that the group operated to support Russian intelligence gathering.  
Source: [http://www.theregister.co.uk/2015/09/17/russian\\_cyberspy\\_dukes\\_campaign/](http://www.theregister.co.uk/2015/09/17/russian_cyberspy_dukes_campaign/)
23. *September 17, Threatpost* – (International) **Dutch police arrest CoinVault ransomware authors.** Dutch authorities arrested two suspects believed to be behind the CoinVault ransomware campaign that started in May 2014 and targeted over 1,500

users in nearly 24 countries. The ransomware encrypted victims' files and made them unrecoverable until payment was received.

Source: <https://threatpost.com/dutch-police-arrest-alleged-coinvault-ransomware-authors/114707/>

24. *September 16, Threatpost* – (International) **Schneider patches plaintext credentials bug in building automation system.** Schneider Electric released a firmware update for its StruxureWare Building Expert automation system addressing a remotely executable vulnerability regarding how the system transmits user credentials in plaintext between server and client machines. The Industrial Control System Cyber Emergency Response Team reported that the vulnerability has not been publicly exploited.

Source: <https://threatpost.com/schneider-patches-plaintext-credentials-bug-in-building-automation-system/114702/>

For another story, see item [5](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

## Communications Sector

25. *September 16, Ars Technica* – (California) **More California fiber optic cable severed as AT&T offers 250K reward.** The FBI is conducting an investigation September 16 into an attack on AT&T data lines in San Francisco after 2 more fiber optic cables were severed September 16, increasing the number of attacks to 16 since July 2014. AT&T is offering \$250,000 for the capture of the culprit.

Source: <http://arstechnica.com/tech-policy/2015/09/more-california-fiber-optic-cable-severed-as-att-offers-250k-reward/>

For another story, see item [20](#)

## Commercial Facilities Sector

26. *September 17, KDVR 31 Denver* – (Colorado) **Arapahoe County condo fire injures at least 16, displaces dozens.** More than 100 people were evacuated and about 16 people were injured after a fire broke out at the Country Club Villas in Arapahoe County September 16. The cause of the fire remains under investigation.

Source: <http://kdvr.com/2015/09/17/several-injured-more-than-100-evacuated-after-arapahoe-county-condominium-fire/>

For another story, see item [24](#)

## **Dams Sector**

Nothing to report



**Department of Homeland Security (DHS)**  
**DHS Daily Open Source Infrastructure Report Contact Information**

**About the reports** - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

**Contact Information**

Content and Suggestions:

Send mail to [cikr.productfeedback@hq.dhs.gov](mailto:cikr.productfeedback@hq.dhs.gov) or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to [support@govdelivery.com](mailto:support@govdelivery.com).

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto:nicc@hq.dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

**Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.